جامعة دمشق

كلية الهندسة المعلوماتية

قسم النظم و الشبكات الحاسوبية

السنة الخامسة



Network Security

أمن الشبكات اللاسلكية

إعداد :

مصطفى محمد نجم

M.N Moustafa-MN@hotmail.com

تعريف أمن الشبكات اللاسلكية :

يعتمد تعريف الأمن إلى حد كبير على السياق، لأن كلمة الأمن تشير إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات .قد نتكلم مثلا عن الأمن عند توصيف الإجراءات الوقائية على الطرق العامة أو عند استعراض نظام حاسوبي جديد يتمتع بمناعة عالية ضد فيروسات البرمجيات .لقد تم تطوير أنظمة عدة لمعالجة الجوانب المختلفة لمفهوم الأمن.

بناء على ذلك فقد قمنا بصياغة مصطلح" أمن الشبكات اللاسلكية "ضمن تصنيف محدد للأمن بغية تسهيل مهمتنا في دراسة الأمن في مجال الشبكات اللاسلكية .يقوم هذا البحث بتعريف أمن الشبكات اللاسلكية ضمن سياق أمن المعلومات، أي أننا عندما نتحدث عن أمن الشبكات اللاسلكية فإننا نعني أمن المعلومات في الشبكات اللاسلكية .

ما هو أمن المعلومات ؟

يشمل أمن المعلومات الخصائص الخمسة التالية :

1. السرية :

التأكيد بأن المعلومات لم تصل لأشخاص، عمليات أو أجهزة غير مخولة بالحصول على هذه المعلومات .

(الحماية من إفشاء المعلومات غير المرخص).

2. التحقق من الهوية :

إجراء أمني للتأكد من صلاحية الاتصال، الرسالة أو المصدر أو وسيلة للتحقق من صلاحية شخص ما لاستقبال معلومات ذات تصنيف محدد (أو التحقق من مصدر هذه المعلومات).

3. الكمال :

تعكس جودة أي نظام للمعلومات مدى صحة و وثوقية نظام التشغيل، التكامل المنطقي للتجهيزات والبرمجيات التي توفر آليات الحماية ومدى تناغم بنى المعلومات مع البيانات المخزنة.

4. التوفر :

الوصول الموثوق إلى البيانات وخدمات المعلومات عند الحاجة إليها من قبل الأشخاص المخولين بذلك.

5. مكافحة الإنكار (المسؤولية):

التأكيد بأن مرسل البيانات قد حصل على إثبات بوصول البيانات إلى المرسل إليه وبأن المستقبل قد حصل على إثبات لشخصية المرسل مما يمنع احتمال إنكار أي من الطرفين بأنه قد عالج هذه البيانات.

تطبيق الخصائص الأمنية في الشبكات اللاسلكية :

ترتبط معايير الشبكات اللاسلكية عادة بالطبقتين الأولى والثانية من بروتوكول OSI دون المساس بالطبقات الأعلى أو حزم بروتوكول الإنترنت IP . يتم نقل" حزم بروتوكول الإنترنت IP ″ ضمن بروتوكولات لاسلكية خاصة بالطبقة الفيزيائية وطبقة ربط البيانات.

على سبيل المثال، إذا ما اعتبرنا ″سرية البيانات المنقولة″ بين نقطتي ولوج فإن تحقيق النتيجة ذاتها (سرية البيانات) يمكن أن يتم عبر عدة أساليب:

- طبقة التطبيقات (عبر بروتوكولات TLS/SSL)
- طبقة بروتوكول الإنترنت IP (عبر بروتوكول IPSEC)
- طبقة ربط البيانات (عبر التشفير اللاسلكي).

عندما نتحدث عن أمن الشبكات اللاسلكية فإننا نعني آليات الأمن المتواجدة ضمن الطبقتين الأولى والثانية، أي التشفير اللاسلكي (على مستوى الوصلة) على سبيل المثال .تشكل آليات الأمن الأخرى المتواجدة ضمن الطبقة الثالثة وما فوقها جزءًا من أمن الشبكة أو أمن التطبيقات.

1. سرية الشبكات اللاسلكية:

- **بروتوكول السرية المكافئة للشبكة السلكية : ″WEP "Wired Equivalent Privacy**

سنعرف سرية الشبكات اللاسلكية بضمان أن المعلومات المرسلة بين نقاط الولوج وحواسب المستخدمين لن تصل إلى أشخاص غير مخولين .يجب أن تضمن سرية الشبكات اللاسلكية بأن الإتصالات الجارية بين مجموعة من نقاط الولوج ضمن نظام توزيع لاسلكي Wireless Distribution System (WDS) أو بين نقطة ولوج AP وحاسب متصل بها STA ستبقى محمية.

لقد ارتبط مفهوم سرية الشبكة اللاسلكية بمصطلح" السرية المكافئة للشبكة السلكية WEP ″ .

وقد شكلت "WEP "Wired Equivalent Privacy جزءًا من المعيار الأساسي IEEE 802.11 للشبكات اللاسلكية في العام 1999.

إن الهدف الرئيس من السرية المكافئة للشبكة السلكية WEP هو تأمين الشبكات اللاسلكية بمستوى من السرية مماثل للسرية المتوفرة في الشبكات السلكية .إن الحاجة إلى هذا البروتوكول كانت جلية :فالشبكات اللاسلكية تستخدم الأمواج اللاسلكية وبالتالي فهي أكثر عرضة لأعين المتطفلين.

لقد كان عمر بروتوكول السرية المكافئة للشبكة السلكية WEP قصيرًا للغاية، فقد أدى تصميمه الرديء وغير الشفاف إلى نجاح العديد من الهجمات في اختراق الشبكات التي تستعمل هذا البروتوكول .لم يستغرق الأمر سوى عدة أشهر من إطلاق البروتوكول حتى تم خرقه وهجرانه .على الرغم من أن طول مفاتيح التشفير كان محدودًا

نتيجة بعض قوانين حظر التصدير إلا أن هذا البروتوكول قد أثبت ضعفه بغض النظر عن طول مفتاح التشفير المستخدم.

لكن العيوب التصميمية لم تكن السبب الوحيد في فشل بروتوكول السرية المكافئة للشبكة السلكية WEP بل أن عدم توفر نظام لإدارة مفاتيح التشفير ضمن نفس البروتوكول قد ساهم أيضًا في إفشاله .لم يتضمن بروتوكول السرية المكافئة للشبكة السلكية WEP أي نظام لإدارة مفاتيح التشفير على الإطلاق، وكانت الوسيلة الوحيدة لتوزيع مفاتيح التشفير تتطلب إعداد / إدخال هذه المفاتيح يدويًا في كل وحدة من التجهيزات اللاسلكية (إلا أن السر المشترك بين عدة أشخاص لم يعد سرًا..!).

أدخل على بروتوكول السرية المكافئة للشبكة السلكية WEP عدد من التعديلات الخاصة ببعض منتجي التجهيزات اللاسلكية إلا أن هذه التعديلات لم ترقى إلى المستوى المطلوب لإنجاح البروتوكول (بعض الأمثلة تتضمن بروتوكول +WEP من شركة Lucent و بروتوكول WEP2 من شركة Cisco).

- **بروتوكولي الوصول المحمي للشبكة اللاسلكية : WPA , WPA2**

بعد موت بروتوكول السرية المكافئة للشبكة السلكية WEP تم اقتراح بروتوكول الوصول المحمي للشبكة WPA في العام 2003 ليتم اعتماده فيما بعد كجزء من معيار الشبكات اللاسلكية IEEE 802.11i عام 2004 تحت اسم WPA2 .

لقد تم تصميم بروتوكولي WPA , WPA2 للعمل مع أو دون وجود مخدم لإدارة مفاتيح التشفير .في حال غياب مخدم إدارة مفاتيح التشفير فإن جميع المحطات ستستخدم" مفتاح تشفير مشترك مسبقًا "Pre-Shared Key PSK" يعرف هذا النمط من التشغيل باسم بروتوكول WPA أو WPA2 الشخصي.

يعرف بروتوكول WPA2 عند استخدام مخدم لمفاتيح التشفير ببروتوكول WPA المؤسساتي .يتطلب بروتوكول WPA2 المؤسساتي وجود مخدم يعمل بمعايير IEEE 802.1X لتوزيع مفاتيح التشفير.

من أهم التطويرات المضمنة في بروتوكول WPA2 مقارنة بسلفه WEP هو إمكانية تبادل مفاتيح التشفير ديناميكيًا بواسطة بروتوكول تكامل مفاتيح التشفير المؤقتة(Temporal Key Integrity Protocol TKIP).

2. التحقق من الهوية في الشبكات اللاسلكية:

يتم تعريف التحقق من الهوية في سياق الشبكات اللاسلكية بالإجراءات الهادفة لضمان صلاحية الإتصال بين نقاط الولوج و/أو المحطات اللاسلكية .يمكن التعبير عن التحقق من الهوية في الشبكات اللاسلكية بشكل أبسط باعتباره حق إرسال البيانات إلى وعبر الشبكة اللاسلكية.

لاستيعاب مفهوم التحقق من الهوية في الشبكات اللاسلكية لا بد من فهم ما يحدث عند بدء جلسة الإتصال بين نقطة ولوج و/أو محطة لاسلكية .يبدأ الإتصال بعملية تدعى" الربط Association" .

لقد تمت إضافة آليتين لعملية" الربط "عند تصميم معيار IEEE 802.11b للشبكات اللاسلكية:

- التحقق المفتوح من الهوية.
- التحقق من الهوية باستخدام المفتاح المشترك.

التحقق المفتوح من الهوية يعني ضمنيًا عدم وجود أي آلية للأمن مما يمكن أي شخص كان من الإتصال مع نقطة الولوج.

تقوم نقطة الولوج في التحقق من الهوية باستخدام المفتاح المشترك بتشارك سر (كلمة سر) مع محطة المستخدم / نقطة الولوج .تتيح آلية طلب الإستجابة للتحدي لنقطة الولوج بالتحقق من أن المستخدم يعرف السر المشترك وستسمح له بالتالي الوصول إلى الشبكة اللاسلكية.

- **إيقاف إرسال معرف مجموعة الخدمات SSID كإجراء لتعزيز أمن الشبكة اللاسلكية:**

طورت شركة Lucent Technologies في العام 2000 نموذجًا مشتقًا من آلية التحقق المفتوح من الهوية أسمتها" الشبكة المغلقة Closed Network". تختلف الشبكات المغلقة عن الشبكات اللاسلكية المعيارية العاملة وفق معيار 802.11b بأنه نقاط الولوج لن ترسل إطارات إرشاد لمعرف مجموعة الخدمات SSID بشكل دوري.

إن إيقاف إرسال معرف مجموعة الخدمات يعني ضمنيًا بأن على مستخدمي الشبكة اللاسلكية الحصول مقدمًا على معرف مجموعة الخدمات الذي يجب استخدامه للربط مع نقطة ولوج (أو مجموعة من نقاط الولوج) لقد تم استخدام هذه الميزة الجديدة من قبل الكثير من مصنعي تجهيزات الشبكات اللاسلكية كإجراء لتعزيز أمن الشبكة .

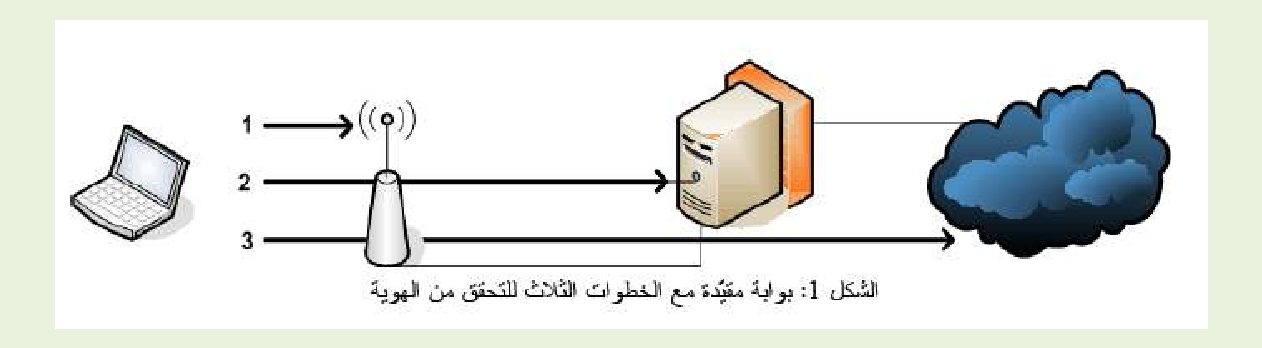
في واقع الأمر فإنه وعلى الرغم من أن إيقاف إرسال معرف مجموعة الخدمات سيمنع المستخدمين غير المخولين من الحصول على هذا المعرف عبر الإطار المرشد، إلا أنها لن تمنع إيجاد معرف مجموعة الخدمات باستخدام برمجيات التجسس على إطارات الربط المرسلة من محطات أخرى .إن إيجاد معرف مجموعة الخدمات لشبكة مغلقة يعني ببساطة انتظار أحد ما ليقوم بالربط بالشبكة اللاسلكية واستخلاص معرف مجموعة الخدمات من إطار الربط المرسل.

- **استخدام فلترة العناوين الفيزيائية MAC كإجراء لتعزيز أمن الشبكة اللاسلكية:**

لقد انتشر استخدام العنوان الفيزيائي لبطاقة الشبكة اللاسلكية كآلية لتحديد أو توفير الوصول إلى الشبكة اللاسلكية بين الكثير من مزودي خدمات الإنترنت اللاسلكية .يعتمد هذا الخيار على اعتبار أن العناوين الفيزيائية MAC مسجلة ضمن المكونات الإلكترونية لبطاقة الشبكة وبالتالي يستحيل تغييرها من قبل المستخدمين العاديين .إلا أن الواقع يخالف هذا الإعتبار، لأنه من الممكن وببساطة تغيير العناوين الفيزيائية في معظم بطاقات الشبكة اللاسلكية (عب طريق إعدادات خاصة و لو أن ذلك التغيير وهمي..!).

- ### البوابات المقيدة للشبكات اللاسلكية:

على الرغم من تعدد أساليب تطبيق البوابات المقيدة للشبكات اللاسلكية إلا أن أغلبها يعتمد على نفس المبدأ. عند استخدام البوابات المقيدة كآلية للتحقق من الهوية في شبكة ما فإن مستخدمي هذه الشبكة سيتمكنون من الربط مع أية نقطة ولوج (دون استخدام آليات التحقق من الهوية في الشبكة اللاسلكية) والحصول على عنوان إنترنت IP عبر بروتوكول الإعداد التلقائي للمضيف DHCP (دون تحقق من هوية المستخدم للحصول على عنوان إنترنت IP) . بعد حصول المستخدم على عنوان إنترنت ستقوم الشبكة بالتقاط جميع طلبات الوصول إلى الإنترنت عبر بروتوكول HTTP لإجبار المستخدم على" تسجيل الدخول "إلى صفحة إنترنت.
تضطلع البوابات المقيدة بمهمة التأكد من صحة كلمة السر التي أدخلها المستخدم وتعديل حالة الجدار الناري.
تعتمد قواعد الجدار الناري على قيم العنوان الفيزيائي MAC و عنوان الانترنت IP الذي حصل عليه المستخدم من DHCP.



الشكل 1: بوابة مقيّدة مع الخطوات الثلاث للتحقق من الهوية

يظهر الشكل السابق الخطوات الثلاث لعملية التحقق من الهوية باستخدام البوابات المقيدة .

- تتطلب الخطوة الأولى أن يتم ربط المستخدم مع الشبكة اللاسلكية .لا تتطلب هذه المرحلة التحقق من هوية المستخدم عبر بروتوكولات WEP/WPA وتقوم الشبكة عادةً بإرسال معرف مجموعة الخدمات SSID.
- في الخطوة الثانية يحصل المستخدم على عنوان إنترنت IP عبر بروتوكول الإعداد التلقائي للمضيف DHCP . تقوم نقطة الولوج بتمرير سيل البيانات IP دون أي تحقق من هوية المستخدم .
- في الخطوة الثالثة و الأخيرة يتم تحويل جميع طلبات الوصول إلى الشبكة عبر بروتوكول HTTP الواردة من الزبون إلى مخدم البوابة المقيدة . يقوم الزبون بتسجيل الدخول إلى المخدم و يتم ذلك عادة بإرسال اسم المستخدم و كلمة المرور عبر بروتوكول HTTPS الآمن. أخيرًا يقوم مخدم البوابة المقيدة بتعديل أو إضافة قاعدة ضمن الجدار الناري للسماح للمستخدم بالوصول إلى الإنترنت.

3. كمال البيانات في الشبكات اللاسلكية:

سنقوم بتعريف كمال البيانات في الشبكات اللاسلكية بقدرة بروتوكول الاتصال اللاسلكي على كشف أي تحريف في البيانات المنقولة من قبل أشخاص غير مخولين.

كان من المفترض ببروتوكول السرية المكافئة للشبكة السلكية WEP في العام 1999 أن يضمن كمال البيانات المنقولة، إلا أن آلية كمال البيانات المستخدمة حينها (التحقق الدوري من الأخطاء CRC) لم تكن آمنة .لقد أتاحت الأخطاء التصميمية في بروتوكول السرية المكافئة للشبكة السلكية WEP إمكانية تعديل البيانات المنقولة وتحديث قيمة CRC الخاصة بهذه البيانات حتى دون معرفة مفتاح تشفير WEP , أي أنه بالإمكان تحريف البيانات المنقولة دون أن يتم يكشف هذا التحريف.

حّلت بروتوكولات WPA و WPA2 مشكلة كمال البيانات الموجودة في سلفها WEP بإضافة شيفرة أكثر أمنًا للتحقق من الرسالة إضافة إلى عداد للإطارات والذي يمنع ما يسمى "هجمات الإعادة Replay Attacks " التي يقوم فيها المهاجم بتسجيل المحادثة بين أحد مستخدمي الشبكة اللاسلكية ونقطة الولوج بغية الحصول على وصول غير مخول إلى هذه الشبكة .بإعادة المحادثة" القديمة "لن يحتاج المهاجم إلى معرفة السر المشترك لـ WEP أو المفتاح.

4. توفر الشبكات اللاسلكية:

سنعرف توفر الشبكة اللاسلكية بقدرة التقنية على ضمان الوصول الموثوق إلى خدمات البيانات والمعلومات للمستخدمين المخولين.

من أول الأمور الواجب أخذها بعين الإعتبار أنه من غير اليسير أن تمنع شخصًا ما من التشويش على إشارة شبكتك اللاسلكية .تعمل الشبكات اللاسلكية ضمن نطاق محدد للقنوات الراديوية يمكن استخدامه من قبل أي شخص لإرسال إشارات لاسلكية .من شبه المستحيل منع الأشخاص غير المخولين من التشويش على شبكتك. غاية ما يمكنك عمله أن تقوم بمراقبة وصلاتك لتحديد المصادر المحتملة للتشويش .

إيقاف الخدمة

تعتبر الشبكات اللاسلكية عرضةً لإيقاف الخدمة Denial of Service (DoS) بسبب التشويش اللاسلكي. خذ على سبيل المثال الحالة التي يقرر بها مشغّل شبكةٍ أخرى إعداد تجهيزاته اللاسلكية لتعمل ضمن نفس القنوات الراديوية المستخدمة في شبكتك. تخيل أيضاً أن هذه الشبكة سترسل نفس معرّف مجموعة الخدمات SSID الخاص بشبكتك.

لتجنب هذه الهجمات المقصودة أو غير المقصودة ينبغي عليك القيام بمسحٍ دوريٍ للترددات اللاسلكية.
لتجنب التشويش على شبكات أخرى يجب عليك ألا تفرط في زيادة طاقة وصلاتك اللاسلكية.

هناك العديد من الأسباب التي قد تخفض من أداء الشبكة اللاسلكية أو توقف عملها بالكامل .قد يتسبب وجود نقاط مخفية في تدن كبير في أداء الشبكات العاملة ببروتوكول IEEE802.11 .

كما قد تتسبب الفيروسات، برمجيات الند للند Peer-to-Peer إضافة إلى الرسائل المرسلة عشوائيًا SPAM وغيرها في تخفيض سعة نقل البيانات المتوفرة للوصول المخول إلى الخدمات الأساسية.

كما ذكرنا في فقرة" التحقق من الهوية "من هذا البحث فإنه من الصعب منع المستخدمين غير المخولين من الاتصال بنقطة الولوج أو البوابة المقيدة الخاصة بك .يتطلب توفر الشبكة اللاسلكية القيام بمهام مراقبة الشبكة بشكلٍ جيد.

5. مكافحة الإنكار (المسؤولية) في الشبكات اللاسلكية :

لا تتعامل معايير الشبكات اللاسكية IEEE802.11 مع (المسؤولية) عن المعلومات المنقولة عبر الشبكة اللاسلكية .

لا تحتوي بروتوكولات الشبكات اللاسلكية على آلية للتأكيد على أن مرسل البيانات قد حصل على إثبات لتسلم المستقبل لرسالته أو على أن المستقبل قد حصل على إثبات لهوية المرسل .لذلك يجب إعداد المسؤولية ضمن بروتوكولات الطبقات العليا.

التهديدات الأمنية للشبكات اللاسلكية:

يظهر الجدول التالي المخاطر الأمنية العشرة الأكثر شيوعا في الشبكات اللاسلكية و يقدم مجموعة من المقترحات لكل منها

1	السرية	خطر التجسس، قد يصل المستخدمون غير المخولين إلى البيانات المنقولة عبر شبكتك اللاسلكية	استخدم التشفير على مستوى الوصلة ضمن وصلاتك اللاسلكية (WPA2). إنصح مستخدمي شبكتك باستخدام "التشفير" ضمن الطبقات ذات المستوى الأعلى (HTTPS, Secure SMTP).
2	السرية	خطر اختطاف البيانات المنقولة، قد يتمكن المستخدمون غير المخولين من تطبيق هجمات الشخص الوسيط	التوصية 1 + راقب نسبة الإشارة إلى الضجيج SNR، معرّف مجموعة الخدمات SSID إضافة إلى العنوان الفيزيائي لنقطة الولوج AP MAC المستخدمة في وصلاتك.
3	التحقق من الهوية	خطر الوصول غير المخول إلى شبكتك اللاسلكية	قم بإعداد بروتوكول IEEE 802.11X (WPA2)). لا تعتمد على أساليب التحقق من الهوية باستخدام العنوان الفيزيائي MAC فقط. لا ترسل معرّف مجموعة الخدمات SSID الخاص بشبكتك.

4	السرية	خطر الوصول غير المخول إلى شبكتك وإلى الإنترنت	قم بإعداد بروتوكول IEEE 802.11X قم بإعداد بوابة مقيدة Captive Portal.
5	التكامل	خطر تحريف البيانات أثناء نقلها لاسلكياً	إنصح مستخدمي شبكتك باستخدام "التشفير" ضمن الطبقات ذات المستوى الأعلى (HTTPS, Secure SMTP). استخدم التشفير على مستوى الوصلة ضمن وصلاتك اللاسلكية (WPA2).
6	التوفر	خطر التشويش اللاسلكي إيقاف عمل الخدمة بسبب التشويش اللاسلكي (التداخل)	راقب طيف الترددات اللاسلكية دورياً. حاذر من الزيادة المفرطة لطاقة وصلاتك.
7	التوفر	خطر انخفاض سعة النقل نتيجة الإرسال المتكرر للإشارات اللاسلكية	تأكد من عدم وجود نقاط مخفية أو مصادر أخرى للتشويش. راقب نقاط الولوج لكشف أية إرسالات متكررة على مستوى الوصلة.
8	التوفر	خطر انخفاض سعة النقل نتيجة البرمجيات المؤذية	راقب البيانات المنقولة لبروتوكول الإنترنت IP وبشكل خاص بروتوكولي ICMP و UDP. ركب أنظمة كشف التسلل Intrusion Detection Systems إذا دعت الحاجة.
9	التحقق من الهوية المسؤولية	خطر الوصول غير المخول لشبكتك الداخلية	قم بتركيب الشبكة اللاسلكية خارج حدود الجدار الناري. استخدم الشبكة الخاصة الإفتراضية VPN واسمح بالوصول إلى شبكتك الداخلية عبر مركز الشبكة الخاصة الإفتراضية فقط.
10	(الوصول إلى الشبكة) المسؤولية	خطر الإستخدام غير المخول لموارد الشبكة والشبكة اللاسلكية	قم بإعداد بروتوكول IEEE 802.11X استخدم البوابات المقيدة المعتمدة على التواقيع الإلكترونية Digital Signature.

جدول التهديدات الأمنية العشرة الأكثر شيوعا في الشبكات اللاسلكية مع نصائح للإجراءات الوقائية

الخلاصة :

لقد استعرضنا خمسة خصائص أمنية :السرية، التحقق من الهوية، الكمال، مكافحة الإنكار والتوفر في سياق الشبكات اللاسلكية.

نظرًا لأن معايير الشبكات اللاسلكية مثل IEEE 802.11 تتعامل فقط مع الطبقتين 1 و 2 من نموذج OSI المعياري فإن من الممكن استخدام بعض الخصائص الأمنية ضمن الطبقات الأعلى أيضًا.

يفترض بالمصمم الجيد للشبكات اللاسلكية أن يفكر مليًا في كيفية إعداد كلٍ من هذه الخصائص الأمنية .على سبيل المثال، قد يقوم بإعداد التشفير من أجل السرية ضمن مستوى الوصلة أو ضمن مستوى التطبيقات أو بروتوكول الإنترنت IP , قد يقوم بإرسال معرف مجموعة الخدمات SSID أو لا , قد يقوم بإعداد التحقق من الهوية باستخدام بروتوكول IEEE 820.1X , يمكن أيضًا استخدام البوابات المقيدة أو التصفية البسيطة والساكنة للعناوين الفيزيائية MAC و غيرها .

ينبغي لأي إعداد لأمن الشبكة أن يعتمد على خصوصية هذه الشبكة وتطبيقاتها

ملاحظات أساسية:

1. يحتوي أمن الشبكات اللاسلكية الصرف على آليات للأمن تعمل ضمن الطبقتين الأولى والثانية فقط.
2. يعتبر التشفير على مستوى الوصلة (WEP, WPA, WPA2) من أكثر إجراءات أمن الشبكة اللاسلكية شيوعًا، إلا أنه لا يضمن السرية المطلقة من بداية الوصلة إلى نهايتها .إذا ما احتجت إلى التشفير على مستوى الوصلة، تجنّب استخدام WEP واستخدم WPA2.
3. لا يمكن اعتبار إيقاف إرسال معرف مجموعة الخدمات SSID أو استخدام تصفية العناوين الفيزيائية MAC وسائل آمنة للتحقق من الهوية .لا بد من استخدام أسلوب للتحقق من الهوية على المستويات الأعلى، كالبوابات المقيدة مثلا.
4. قد تتوقف الشبكة اللاسلكية عن العمل نتيجة هجمات متعمدة لإيقاف عمل الخدمة DOS أو وجود برمجيات مؤذية، كما أن الشبكة قد تتعطل دون قصد بسبب وجود نقاط خفية أو مشاكل تشويش .لن تتمكن من اكتشاف الأسباب الحقيقية وراء هذه المشاكل إلا من خلال مراقبة سير البيانات عبر شبكتك.
5. لا يوجد" حل أمني قياسي "يلائم جميع الشبكات اللاسلكية .من الضروري تحديد المتطلبات الأمنية بوضوح لأن الحلول تعتمد على خصوصية كل حالة.

تم بعونه تعالى

M.N Moustafa-MN@hotmail.com

- **Reference :**

- www.itrainonline.org/itrainonline/mmtk
- http://telecom.gmu.edu/publications/Kieth-Fleming-Wireless-Security-Project-f2-May-2005.doc
- http://www.invictusnetworks.com/faq/Securing%20Wireless%20LAN/Wi-Fi_ProtectedAccessWebcast_2003.pdf
- http://www.wi-fi.org/getfile.asp?f=Whitepaper_Wi-Fi_Security4-29-03.pdf